07.10.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

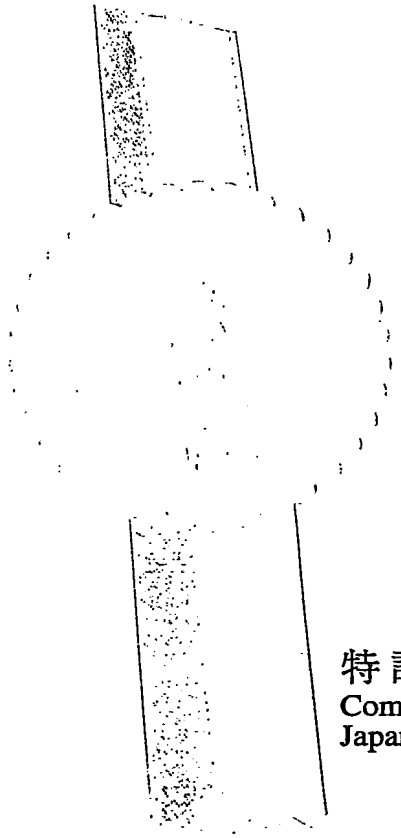
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１０月２８日

出願番号
Application Number: 特願２００３－３６７５２７

[ST. 10/C]: [ＪＰ２００３－３６７５２７]

出願人
Applicant(s): 財団法人生産技術研究奨励会



２００４年１１月１２日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３１０２３７２

【書類名】　特許願
【整理番号】　IIS03014
【提出日】　平成15年10月28日
【あて先】　特許庁長官　殿
【国際特許分類】　B65C　9/00
【発明者】
　【住所又は居所】　神奈川県横浜市戸塚区品濃町５５７－４４－２０５
　【氏名】　今井　秀樹
【発明者】
　【住所又は居所】　東京都三鷹市大沢２－２０－３１－１－４０２
　【氏名】　古原　和邦
【発明者】
　【住所又は居所】　東京都目黒区駒場四丁目６番１号　東京大学生産技術研究所内
　【氏名】　辛　星漢
【特許出願人】
　【識別番号】　801000049
　【氏名又は名称】　財団法人生産技術研究奨励会
【代理人】
　【識別番号】　100064908
　【弁理士】
　【氏名又は名称】　志賀　正武
【選任した代理人】
　【識別番号】　100108578
　【弁理士】
　【氏名又は名称】　高橋　詔男
【選任した代理人】
　【識別番号】　100089037
　【弁理士】
　【氏名又は名称】　渡邊　隆
【選任した代理人】
　【識別番号】　100101465
　【弁理士】
　【氏名又は名称】　青山　正和
【選任した代理人】
　【識別番号】　100094400
　【弁理士】
　【氏名又は名称】　鈴木　三義
【選任した代理人】
　【識別番号】　100107836
　【弁理士】
　【氏名又は名称】　西　和哉
【選任した代理人】
　【識別番号】　100108453
　【弁理士】
　【氏名又は名称】　村山　靖彦
【手数料の表示】
　【予納台帳番号】　008707
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1

【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0203645

【書類名】特許請求の範囲
【請求項１】
端末装置とサーバ間において相互に認証を行う認証システムであって、
前記端末装置は、
ユーザが予め決定しておいたパスワードに基づいて、サーバ登録用のパスワード認証データＨとユーザ保存用の認証情報Ｐ’を求めるデータ伸長手段と、
前記データ伸長手段によって求めた認証情報Ｐ’を予め記憶しておく記憶手段と、
前記記憶手段から読み出した認証情報Ｐ’と認証時に入力されたパスワードを入力として所定の計算式により値Ｐを求める結合手段と、
前記値Ｐと内部において発生させた乱数を入力として所定の計算式により値Ｙ１を求め、前記サーバへ送信するマスク演算手段と、
前記値Ｐと内部において発生させた乱数と前記サーバから受信した値Ｙ２を入力として所定の計算式により値ＭＫを求めるマスター鍵生成手段と、
前記値ＭＫを入力として所定の計算式により値Ｖ１を求め、サーバへ送信するとともに、前記サーバから受信した値Ｖ２と値Ｖ１と比較照合し、一致した場合にサーバを認証する認証結果判断手段と
を備え、
前記サーバは、
前記データ伸長手段によって求めたパスワード認証データＨを予め記憶しておく記憶手段と、
前記記憶手段から読み出したパスワード認証データＨと内部において発生させた乱数を入力として所定の計算式により値Ｙ２を求め、前記端末装置へ送信するマスク演算手段と、
前記パスワード認証データＨと内部において発生させた乱数と前記端末装置から受信した値Ｙ１を入力として所定の計算式により値ＭＫを求めるマスター鍵生成手段と、
前記値ＭＫを入力として所定の計算式により値Ｖ２を求め、端末装置へ送信するとともに、前記端末装置から受信した値Ｖ１と値Ｖ２と比較照合し、一致した場合に端末装置を認証する認証結果判断手段と
を備えたことを特徴とする認証システム。
【請求項２】
前記端末装置及びサーバは、相互の認証が行われた場合に、セッション鍵を生成するセッション鍵生成手段をそれぞれに備えたことを特徴とする請求項１に記載の認証システム。
【請求項３】
前記認証情報Ｐ’は、多項式であることを特徴とする請求項１または２に記載の認証システム。
【請求項４】
前記認証情報Ｐ’は、ハッシュ関数であることを特徴とする請求項１または２に記載の認証システム。
【請求項５】
前記認証情報Ｐ’は、疑似乱数関数であることを特徴とする請求項１または２に記載の認証システム。
【請求項６】
端末装置とサーバ間において相互に認証を行う認証システムにおける端末装置上で動作する認証プログラムであって、
ユーザが予め決定しておいたパスワードに基づいて、サーバ登録用のパスワード認証データＨとユーザ保存用の認証情報Ｐ’を求めるデータ伸長処理と、
前記データ伸長処理によって求めた認証情報Ｐ’を予め記憶しておく記憶処理と、
前記記憶処理により記憶しておいた認証情報Ｐ’と認証時に入力されたパスワードを入力として所定の計算式により値Ｐを求める結合処理と、

前記値Ｐと内部において発生させた乱数を入力として所定の計算式により値Ｙ１を求め、前記サーバへ送信するマスク演算処理と、
前記値Ｐと内部において発生させた乱数と前記サーバから受信した値Ｙ２を入力として所定の計算式により値ＭＫを求めるマスター鍵生成処理と、
前記値ＭＫを入力として所定の計算式により値Ｖ１を求め、サーバへ送信するとともに、前記サーバから受信した値Ｖ２と値Ｖ１と比較照合し、一致した場合にサーバを認証する認証結果判断処理と
をコンピュータに行わせることを特徴とする認証プログラム。
【請求項７】
相互の認証が行われた場合に、セッション鍵を生成するセッション鍵生成処理をさらにコンピュータに行わせることを特徴とする請求項６に記載の認証プログラム。
【請求項８】
端末装置とサーバ間において相互に認証を行う認証システムにおけるサーバ上で動作する認証プログラムであって、
パスワード認証データＨを予め記憶しておく記憶処理と、
前記記憶処理により記憶しておいたパスワード認証データＨと内部において発生させた乱数を入力として所定の計算式により値Ｙ２を求め、前記端末装置へ送信するマスク演算処理と、
前記パスワード認証データＨと内部において発生させた乱数と前記端末装置から受信した値Ｙ１を入力として所定の計算式により値ＭＫを求めるマスター鍵生成処理と、
前記値ＭＫを入力として所定の計算式により値Ｖ２を求め、端末装置へ送信するとともに、前記端末装置から受信した値Ｖ１と値Ｖ２と比較照合し、一致した場合に端末装置を認証する認証結果判断処理と
をコンピュータに行わせることを特徴とする認証プログラム。
【請求項９】
相互の認証が行われた場合に、セッション鍵を生成するセッション鍵生成処理をさらにコンピュータに行わせることを特徴とする請求項８に記載の認証プログラム。
【請求項１０】
前記認証情報Ｐ’は、多項式であることを特徴とする請求項６ないし９のいずれかに記載の認証プログラム。
【請求項１１】
前記認証情報Ｐ’は、ハッシュ関数であることを特徴とする請求項６ないし９のいずれかに記載の認証プログラム。
【請求項１２】
前記認証情報Ｐ’は、疑似乱数関数であることを特徴とする請求項６ないし９のいずれかに記載の認証プログラム。

【書類名】明細書
【発明の名称】認証システム
【技術分野】
【０００１】
本発明は、認証に関する情報の漏洩に強い認証システムに関する。
【背景技術】
【０００２】
従来からユーザの端末装置とサーバとの間において認証を行う方法として、ユーザＩＤとユーザのみが知っているパスワードとを端末装置から入力し、サーバ側に蓄えられている情報と一致すれば、正当なユーザであることを認証する方法が知られている。
しかし、この方法は、端末装置とサーバ間の通信経路中において、不正にこれらの情報が盗まれてしまうと、簡単に不正利用を許してしまうため、ＳＳＬ（非特許文献１）、ＴＬＳ（非特許文献２）、ＳＳＨ（非特許文献３）等の暗号化技術を用いて、情報の送受信を行うのが一般的である。これは、パスワードと秘密の値と公開されている値とを使用して認証を行うものである。

【非特許文献１】A.Frier,P.Karlton,and P.Kocher.The SSL 3.0 Protocol.Netscape Communications Corp.,1996,http://wp.netccape.com/eng/ssl3/
【非特許文献２】IETF(Internet Engineering Task Force).Transport Layer security (tls) Charter.http://www.ietf.org/html.charters/tls-charter.html
【非特許文献３】IETF(Internet Engineering Task Force).Secure Shell(secsh)Charter.http://www.ietf.org/html.charters/secsh-charter.html

【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかしながら、非特許文献１～３に示す方法は、ユーザ側から暗号化された情報が漏れた場合は、オフラインの解析作業によってパスワードを求めることができてしまうという問題がある。サーバに対してオンラインでパスワード入力を繰り返し行う方法は、パスワードを間違えた回数に応じてアクセスを拒否するなどの対策を講じることが可能であるが、オフラインの解析作業は、防止策を講じることができないという問題もある。
【０００４】
本発明は、このような事情に鑑みてなされたもので、情報の漏洩に強く、安全に暗号鍵の交換を行うことができる認証システムを提供することを目的とする。
【課題を解決するための手段】
【０００５】
請求項１に記載の発明は、端末装置とサーバ間において相互に認証を行う認証システムであって、前記端末装置は、ユーザが予め決定しておいたパスワードに基づいて、サーバ登録用のパスワード認証データＨとユーザ保存用の認証情報Ｐ’を求めるデータ伸長手段と、前記データ伸長手段によって求めた認証情報Ｐ’を予め記憶しておく記憶手段と、前記記憶手段から読み出した認証情報Ｐ’と認証時に入力されたパスワードを入力として所定の計算式により値Ｐを求める結合手段と、前記値Ｐと内部において発生させた乱数を入力として所定の計算式により値Ｙ１を求め、前記サーバへ送信するマスク演算手段と、前記値Ｐと内部において発生させた乱数と前記サーバから受信した値Ｙ２を入力として所定の計算式により値ＭＫを求めるマスター鍵生成手段と、前記値ＭＫを入力として所定の計算式により値Ｖ１を求め、サーバへ送信するとともに、前記サーバから受信した値Ｖ２と値Ｖ１と比較照合し、一致した場合にサーバを認証する認証結果判断手段とを備え、前記サーバは、前記データ伸長手段によって求めたパスワード認証データＨを予め記憶しておく記憶手段と、前記記憶手段から読み出したパスワード認証データＨと内部において発生させた乱数を入力として所定の計算式により値Ｙ２を求め、前記端末装置へ送信するマスク演算手段と、前記パスワード認証データＨと内部において発生させた乱数と前記端末装置から受信した値Ｙ１を入力として所定の計算式により値ＭＫを求めるマスター鍵生成手

段と、前記値ＭＫを入力として所定の計算式により値Ｖ２を求め、端末装置へ送信するとともに、前記端末装置から受信した値Ｖ１と値Ｖ２と比較照合し、一致した場合に端末装置を認証する認証結果判断手段とを備えたことを特徴とする。

【０００６】

請求項２に記載の発明は、前記端末装置及びサーバは、相互の認証が行われた場合に、セッション鍵を生成するセッション鍵生成手段をそれぞれに備えたことを特徴とする。

【０００７】

請求項３に記載の発明は、前記認証情報Ｐ’は、多項式であることを特徴とする。

【０００８】

請求項４に記載の発明は、前記認証情報Ｐ’は、ハッシュ関数であることを特徴とする。

【０００９】

請求項５に記載の発明は、前記認証情報Ｐ’は、疑似乱数関数であることを特徴とする。

【００１０】

請求項６に記載の発明は、端末装置とサーバ間において相互に認証を行う認証システムにおける端末装置上で動作する認証プログラムであって、ユーザが予め決定しておいたパスワードに基づいて、サーバ登録用のパスワード認証データＨとユーザ保存用の認証情報Ｐ’を求めるデータ伸長処理と、前記データ伸長処理によって求めた認証情報Ｐ’を予め記憶しておく記憶処理と、前記記憶処理により記憶しておいた認証情報Ｐ’と認証時に入力されたパスワードを入力として所定の計算式により値Ｐを求める結合処理と、前記値Ｐと内部において発生させた乱数を入力として所定の計算式により値Ｙ１を求め、前記サーバへ送信するマスク演算処理と、前記値Ｐと内部において発生させた乱数と前記サーバから受信した値Ｙ２を入力として所定の計算式により値ＭＫを求めるマスター鍵生成処理と、前記値ＭＫを入力として所定の計算式により値Ｖ１を求め、サーバへ送信するとともに、前記サーバから受信した値Ｖ２と値Ｖ１と比較照合し、一致した場合にサーバを認証する認証結果判断処理とをコンピュータに行わせることを特徴とする。

【００１１】

請求項７に記載の発明は、相互の認証が行われた場合に、セッション鍵を生成するセッション鍵生成処理をさらにコンピュータに行わせることを特徴とする。

【００１２】

請求項８に記載の発明は、端末装置とサーバ間において相互に認証を行う認証システムにおけるサーバ上で動作する認証プログラムであって、パスワード認証データＨを予め記憶しておく記憶処理と、前記記憶処理により記憶しておいたパスワード認証データＨと内部において発生させた乱数を入力として所定の計算式により値Ｙ２を求め、前記端末装置へ送信するマスク演算処理と、前記パスワード認証データＨと内部において発生させた乱数と前記端末装置から受信した値Ｙ１を入力として所定の計算式により値ＭＫを求めるマスター鍵生成処理と、前記値ＭＫを入力として所定の計算式により値Ｖ２を求め、端末装置へ送信するとともに、前記端末装置から受信した値Ｖ１と値Ｖ２と比較照合し、一致した場合に端末装置を認証する認証結果判断処理とをコンピュータに行わせることを特徴とする。

【００１３】

請求項９に記載の発明は、相互の認証が行われた場合に、セッション鍵を生成するセッション鍵生成処理をさらにコンピュータに行わせることを特徴とする。

【００１４】

請求項１０に記載の発明は、前記認証情報Ｐ’は、多項式であることを特徴とする。

【００１５】

請求項１１に記載の発明は、前記認証情報Ｐ’は、ハッシュ関数であることを特徴とする。

【００１６】

請求項１２に記載の発明は、前記認証情報Ｐ’は、疑似乱数関数であることを特徴とする。

【発明の効果】

【００１７】

この発明によれば、端末装置側あるいはサーバ側から装置内に保存している情報が漏れたとしてもオフライン解析によってパスワードを見つけだすことができないため、サーバの不正利用を防止することが可能になるという効果が得られる。また、装置内に保存されいる情報を盗まれないようにするための耐タンパー性のモジュールを使用する必要がないため、装置構成を簡単にすることができる。また、公開鍵暗号システムのように複雑な鍵管理処理を行う必要がないため、計算処理を向上させることができるとともに、処理内容を簡単にすることができる。

【発明を実施するための最良の形態】

【００１８】

以下、本発明の一実施形態による認証システムを図面を参照して説明する。この認証システムは、ユーザの端末装置とサーバの認証装置がお互いに相互認証しながら同じセッション鍵を確保するためのシステムである。

ここで、以下の説明において用いる記号について説明しておく。

ｐ，ｑは素数であり、ｑ｜ｐ－１という関係がある。また、ｇ，ｈはｍｏｄｐ上の位数ｑの有限体(群)Ｇの生成元である（楕円曲線上の群でも同じように構成できる）。ここで、ｇは(１＜ｇ＜ｐ－１，$g^a = 1 \bmod p$)であり、ｈは$h = g^q \bmod p$である。つまり、ｐ，ｑは演算体系を示す。例えば、$H = h^x \bmod p$ $(0 \leqq x < q)$でｘは秘密情報である（$x = \log_h H$；Ｈの生成元ｈに対する離散対数）。また、乱数発生器から発生される乱数はＲ∈Ｚ／ｑＺを無作為に生成する。

【００１９】

＜端末装置初期化＞

ユーザは、サーバに対して個人登録したい時、自分の端末装置の初期化を行う。図１は、ユーザの端末装置の初期化処理の構成を示すブロック図である。初期化は、ユーザがパスワードを入力すると、データ伸張器１１によって、サーバ登録用のパスワード認証データＨと、ユーザ保存用の値Ｐ’が生成され、パスワード認証データＨは、サーバに受け渡され、値Ｐ’は、メモリ１２へ保存する。ここで、データ伸長器１１は、（１）多項式、（２）ハッシュ関数、（３）擬似乱数発生器などで構成することが可能である。

【００２０】

（１）多項式を利用する場合

初めに、図２を参照して、多項式を利用する場合について説明する。

まず、多項式発生器１１１によりランダムに多項式を発生する。このとき、登録するサーバの数が一つだったら１次多項式をｎだったらｎ次多項式を発生する。例えば、一つのサーバの場合、ｐ’（ｘ）は、$p'(x) = \alpha_1 \cdot x \bmod q$となる。ここで、ユーザは自分が覚えているパスワード（例えば、”Ｐｏｏｈ９３”）を入力する。多項式とユーザのパスワードが入力されたらパスワード認証データ生成器１１２は、パスワード認証データＨを生成する。パスワード認証データＨは、例えば$H = h^{p'(1)+Pooh93} \bmod p$によりに計算できる。ここで、ｐ’（１）はｐ’（ｘ）でｘの代わりにサーバのＩＤ（例えば、「１」）入れて計算した値である。パスワード認証データＨはユーザが直接にサーバに渡したり、郵便で送付したり、あるいは電話で知らせるなどして、安全に通知する必要がある。ユーザの端末装置の内部にあるメモリ１２は多項式発生器から発生された多項式Ｐ’＝ｐ’（ｘ）を記憶して保存する。

【００２１】

（２）ハッシュ関数を利用する場合

次に、図３を参照して、ハッシュ関数を利用する場合について説明する。

まず、ハッシュ関数発生器１１３によりランダムにハッシュ関数ＨＡＳＨを発生する。そして、秘密値発生器１１４もランダムに秘密値Ｓを発生する。ここで、ユーザは自分が

覚えているパスワード（例えば、”Ｐｏｏｈ９３”）を入力する。ハッシュ関数ＨＡＳＨと秘密値Ｓとユーザのパスワードが入力されたらパスワード認証データ生成器１１５はパスワード認証データＨを生成する。Ｈは、$H=h^{HASH(S\|Pooh93\|1)} \bmod p$により計算できる。ここで、「１」はサーバのＩＤを表す。パスワード認証データＨはユーザが直接にサーバに渡したり、郵便で送付したり、あるいは電話で知らせるなどして、安全に通知する必要がある。ユーザの端末装置の内部にあるメモリ１２はハッシュ関数発生器１１３と秘密値発生器１１４から発生されたハッシュ関数ＨＡＳＨと秘密値Ｓとを一緒にＰ’＝（ＨＡＳＨ，Ｓ）として記憶して保存する。

【００２２】

（３）擬似乱数発生器を利用する場合

次に、図４を参照して、擬似乱数発生器を利用する場合について説明する。

まず、擬似乱数発生器１１６によりランダムに擬似乱数関数ＰＲＮＧを発生する。そして、秘密値発生器１１７もランダムに秘密値Ｓを発生する。ここで、ユーザは自分が覚えているパスワード（例えば、”Ｐｏｏｈ９３”）を入力する。擬似乱数関数ＰＲＮＧと秘密値Ｓとユーザのパスワードが入力されたのを受けて、パスワード認証データ生成器１１８はパスワード認証データＨを生成する。Ｈは、$H=h^{PRNG(S\|Pooh93\|1)} \bmod p$により計算できる。ここで、「１」はサーバのＩＤを表す。パスワード認証データＨはユーザが直接にサーバに渡したり、郵便で送付したり、あるいは電話で知らせるなどして、安全に通知する必要がある。ユーザの端末装置の内部にあるメモリ１２は擬似乱数発生器１１６と秘密値発生器１１７から発生させた擬似乱数関数ＰＲＮＧと秘密値Ｓを一緒にＰ’＝（ＰＲＮＧ，Ｓ）として記憶して保存する。

【００２３】

次に、図６、７を参照して、前述した初期化を行った端末装置１とサーバ２（図５参照）との間で相互認証及び鍵交換を行う動作を説明する。

【００２４】

＜端末装置の動作＞

（１）多項式を利用した場合

初めに、多項式を利用した場合の端末装置１の動作を説明する。

まず、ユーザの端末装置１に備えたメモリ１２から記憶された多項式Ｐ’＝ｐ’（ｘ）を読み出す。結合器３２はメモリ１２から読み出した多項式Ｐ’とユーザが入力したパスワードによりＰ＝ｐ（ｘ）を計算して出力する。例えば、ｐ（ｘ）＝ｐ’（ｘ）＋Ｐｏｏｈ９３＝α_1・ｘ＋Ｐｏｏｈ９３ｍｏｄｑにより計算する。マスク演算器３４は、結合器３２から入力されたＰと乱数発生器３３において発生させた乱数R_1とからY_1を、$Y_1=g^{R_1}\cdot h^{-P(I)} \bmod p$により計算する。ここでｐ（１）は、ｐ（１）＝ｐ’（１）＋Ｐｏｏｈ９３＝α_1・１＋Ｐｏｏｈ９３ｍｏｄｑにより計算する。ここで、「１」はサーバの認証ＩＤを表す。通信処理部３５はY_1をサーバ２へ送信し、サーバ２からY_2を受信する。マスター鍵生成器３６は結合器３２から出力されるＰと乱数発生器３３から出力されるR_1と受信したY_2を入力としてＭＫを、$MK=(Y_2\cdot h^{-P(1)})^{R1} \bmod p$により計算して出力する。

【００２５】

続いて認証結果判断部３７は、ＭＫを入力として、V_1＝ＨＡＳＨ（００‖Y_1‖Y_2‖ＭＫ）によりV_1を計算してこのV_1を通信処理部３５によりサーバ２へ送信し、サーバ２から受信したV_2とV_1を比較する。ここで、ＨＡＳＨは一方向ハッシュ関数である。

【００２６】

次に、認証結果判断部３７においてV_2とV_1が一致しない場合、認証結果判断部３７は、エラー発生器３８に対して、一致しないことを通知する。これを受けて、エラー発生器３８はエラーを発生して処理を中断する。一方、認証結果判断部３７においてV_2とV_1が一致した場合はサーバ２が正当な装置として認証してセッション鍵生成器３９は、ＳＫ＝ＨＡＳＨ（１１‖Y_1‖Y_2‖ＭＫ)によりセッション鍵ＳＫを生成する。

【００２７】

（２）ハッシュ関数を利用した場合

次に、ハッシュ関数を利用した場合の端末装置１の動作を説明する。

まず、ユーザの端末装置１に備えたメモリ１２から記憶されたP'（ＨＡＳＨ,Ｓ）を読み出す。ここで、ＨＡＳＨはハッシュ関数、Ｓは秘密値である。結合器３２はメモリ１２から読み出したP'とユーザが入力したパスワードによりＰ＝ｐ（ｘ）を計算して出力する。例えば、ｐ（ｘ）＝ＨＡＳＨ（Ｓ‖Ｐｏｏｈ９３‖ｘ）ｍｏｄｑにより計算する。マスク演算器３４は、結合器３２から入力されたＰと乱数発生器３３において発生させた乱数R_1とからY_1を、$Y_1=g^{R1}\cdot h^{-p(1)}$ ｍｏｄｑにより計算する。ここで、ｐ（１）は、ｐ（１）＝ＨＡＳＨ（Ｓ‖Ｐｏｏｈ９３‖１）ｍｏｄｑにより計算する。ここで、「１」はサーバのＩＤを表す。通信処理部３５は、Y_1をサーバ２へ送信し、サーバ２からY_2を受信する。マスター鍵生成器３６は結合器３２から出力されるＰと乱数発生器３３から出力されるR_1と受信したY_2を入力としてＭＫを、$MK=(Y_2\cdot h^{-P(1)})^{R1}$ ｍｏｄｐにより計算して出力する。

【００２８】

続いて認証結果判断部３７は、ＭＫを入力として、V_1＝ＨＡＳＨ（００‖Y_1‖Y_2‖ＭＫ）によりV_1を計算してこのV_1を通信処理部３５によりサーバ２へ送信し、サーバ２から受信したV_2とV_1を比較する。ここで、ＨＡＳＨは一方向ハッシュ関数である。

【００２９】

次に、認証結果判断部３７においてV_2とV_1が一致しない場合、認証結果判断部３７は、エラー発生器３８に対して、一致しないことを通知する。これを受けて、エラー発生器３８はエラーを発生して処理を中断する。一方、認証結果判断部３７においてV_2とV_1が一致した場合はサーバ２が正当な装置として認証してセッション鍵生成器３９は、ＳＫ＝ＨＡＳＨ（１１‖Y_1‖Y_2‖ＭＫ)によりセッション鍵ＳＫを生成する。

【００３０】

（３）擬似乱数発生器を利用した場合

次に、疑似乱数関数を利用した場合の端末装置１の動作を説明する。

疑似乱数関数を利用した場合は、メモリ１２に記憶されたハッシュ関数ＨＡＳＨの代わりに疑似乱数関数ＰＲＮＧを用いる以外は、ハッシュ関数を利用した場合と同様の動作であるため、ここでは詳細な説明を省略する。

【００３１】

＜サーバの動作＞

サーバ２は、前述した多項式利用した場合、ハッシュ関数利用した場合、擬似乱数利用した場合に関わらず次のように動作する。

サーバ２に備えたメモリ４１に保存されたユーザＩＤとパスワードの認証データＨを読み出す。マスク演算器４３はメモリ４１から読み出したＨと乱数発生器４２から発生させた乱数R_2を入力としてY_2を、$Y_2=g^{R2}\cdot H=g^{R2}\cdot h^{p(1)}$ ｍｏｄｐにより計算する。通信処理部４４は、計算して得られたY_2を端末装置１に送信し、端末装置１から受信したY_1をマスター鍵生成器４５へ出力する。マスク鍵生成器４５はメモリ４１から読み出したＨと乱数発生器４２からのR_2と通信処理部４４からのY_1を入力としてＭＫを、$MK=(Y_1\cdot h^{p(1)})^{R2}$ ｍｏｄｐにより計算して、ＭＫを出力する。

【００３２】

続いて認証結果判断部４６は、ＭＫを入力として、V_2＝ＨＡＳＨ（００‖Y_1‖Y_2‖ＭＫ）によりV_2を計算してこのV_2を通信処理部４４により端末装置１へ送信し、端末装置１から受信したV_1とV_2を比較する。ここで、ＨＡＳＨは一方向ハッシュ関数である。

【００３３】

次に、認証結果判断部４６においてV_1とV_2が一致しない場合、認証結果判断部４６は、エラー発生器４７に対して、一致しないことを通知する。これを受けて、エラー発生器４７はエラーを発生して処理を中断する。一方、認証結果判断部４６においてV_1とV_2が一致した場合は端末装置１が正当な装置として認証してセッション鍵生成器４８は、

ＳＫ＝ＨＡＳＨ（１１‖Y_1‖Y_2‖ＭＫ)によりセッション鍵ＳＫを生成する。

【００３４】

このように、多項式を利用することにより、不正利用しようと思っている者が他人の端末装置を持っていたとしてもユーザのパスワードは情報理論的に安全である。また、サーバ内に侵入して保存されている情報を得たとしてもユーザのパスワードは情報理論的に安全である。また、ハッシュ関数と擬似乱数発生器を利用する場合には、不正利用しようと思っている者にとってユーザのパスワードは計算量的に安全である。

【００３５】

なお、図１における処理部の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより認証処理、鍵交換処理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。また、「コンピュータシステム」は、ホームページ提供環境（あるいは表示環境）を備えたＷＷＷシステムも含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。

【００３６】

また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【図面の簡単な説明】

【００３７】

【図１】本発明の一実施形態における端末装置の構成を示すブロック図である。
【図２】図１に示すデータ伸長器１１の構成を示すブロック図である。
【図３】図１に示すデータ伸長器１１の構成を示すブロック図である。
【図４】図１に示すデータ伸長器１１の構成を示すブロック図である。
【図５】相互認証及び鍵交換を行う装置の構成を示すブロック図である。
【図６】図５に示す端末装置１の構成を示すブロック図である。
【図７】図５に示すサーバ２の構成を示すブロック図である。

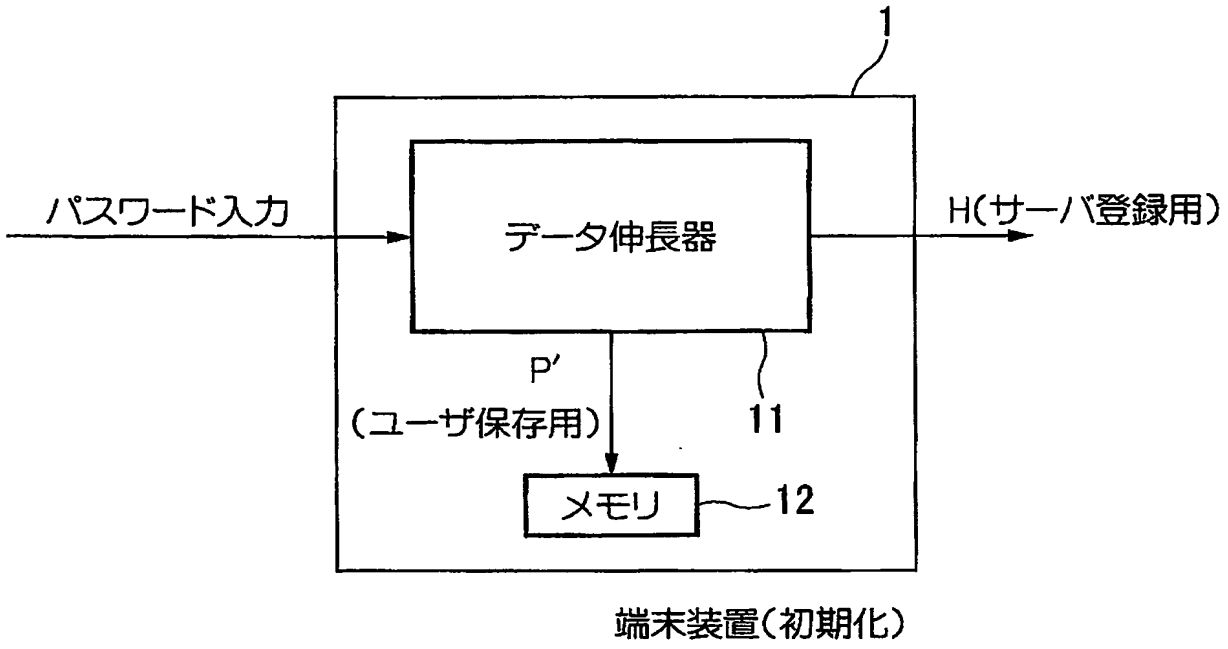
【符号の説明】

【００３８】

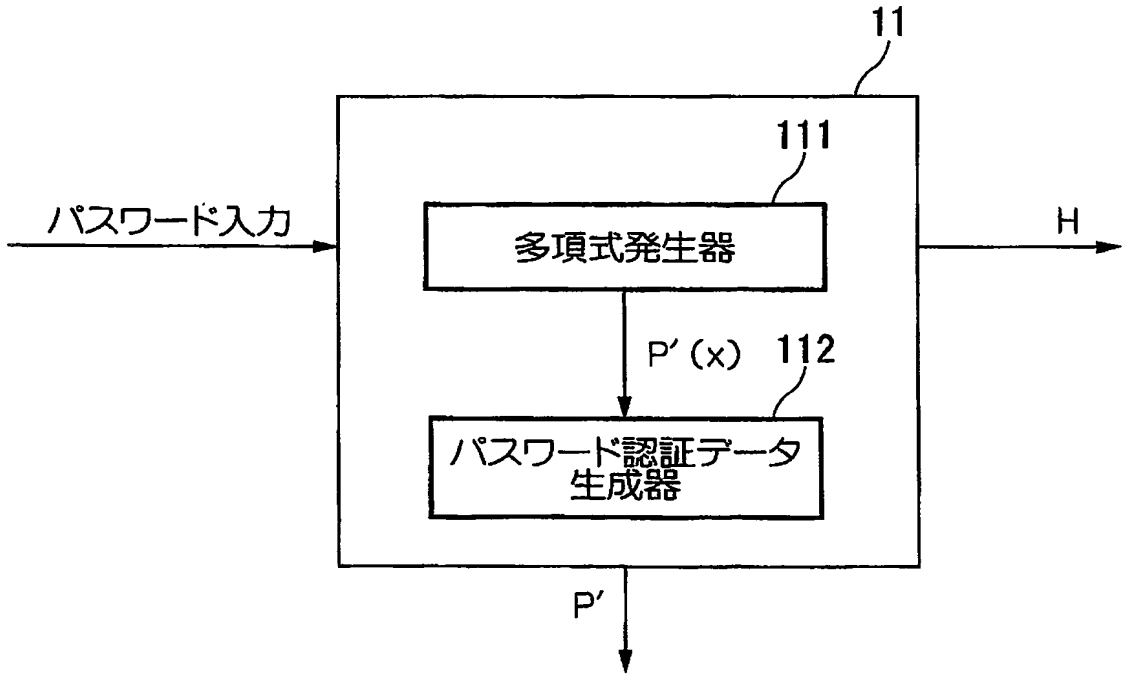
１・・・端末装置、
１１・・・データ伸長器、
１１１・・・多項式発生器、
１１２・・・パスワード認証データ生成器、
１１３・・・ハッシュ関数発生器、
１１４・・・秘密値発生器、
１１５・・・パスワード認証データ生成器、
１１６・・・疑似乱数発生器、
１１７・・・秘密値発生器、
１１８・・・パスワード認証データ生成器、
１２・・・メモリ、
３２・・・結合器、
３３・・・乱数発生器、
３４・・・マスク演算器、
３５・・・通信処理部、
３６・・・マスター鍵生成器、
３７・・・認証結果判断部、
３８・・・エラー発生器、
３９・・・セッション鍵生成器、
２・・・サーバ、

４１・・・メモリ、
４２・・・乱数発生器、
４３・・・マスク演算器、
４４・・・通信処理部、
４５・・・マスター鍵生成器、
４６・・・認証結果判断部、
４７・・・エラー発生器、
４８・・・セッション鍵生成器

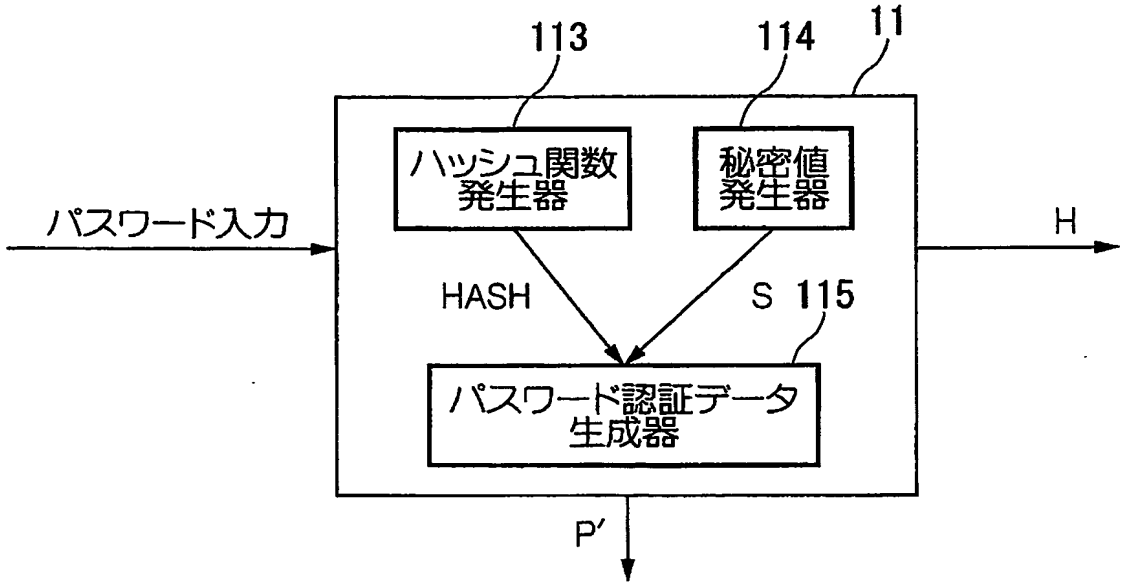
【書類名】図面
【図１】


1
パスワード入力
データ伸長器
H(サーバ登録用)
P′
(ユーザ保存用)
11
メモリ
12
端末装置(初期化)

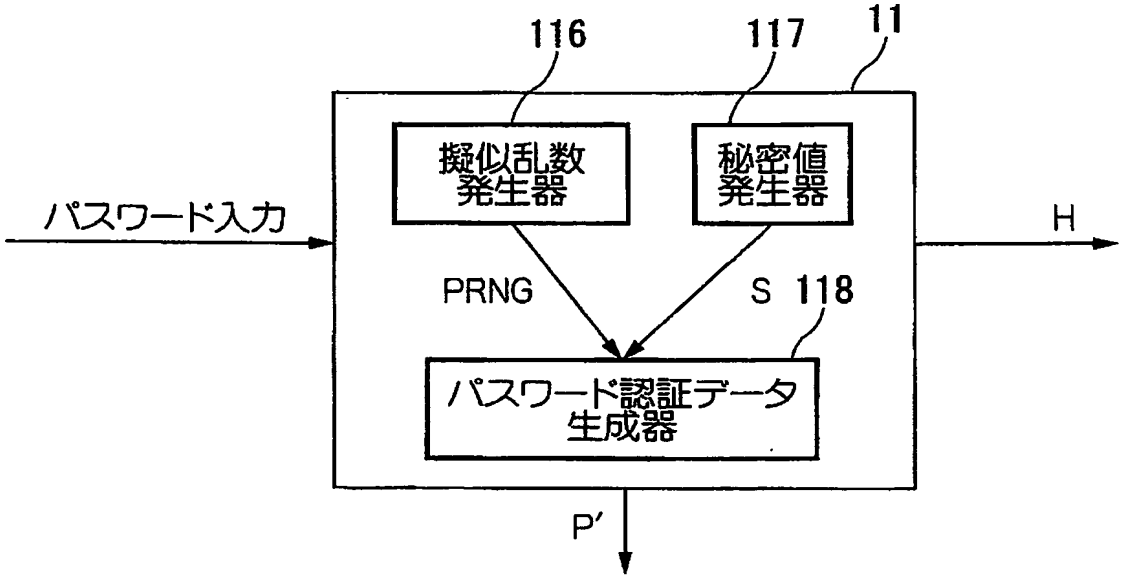
【図２】


11
111
パスワード入力
多項式発生器
H
P′(x)
112
パスワード認証データ
生成器
P′

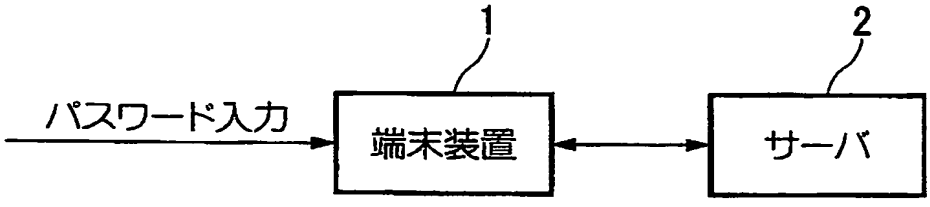
【図３】



【図４】

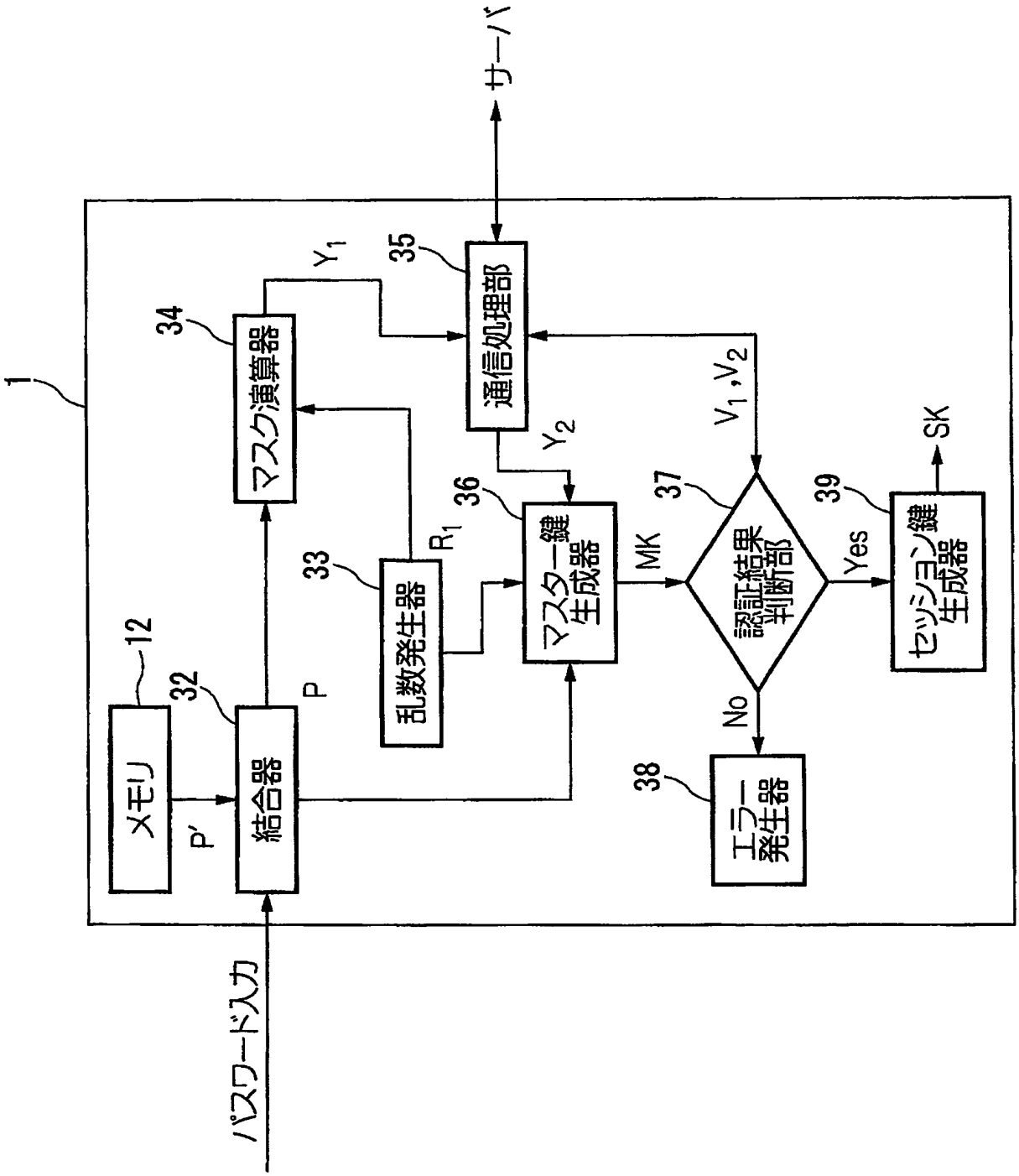


【図５】

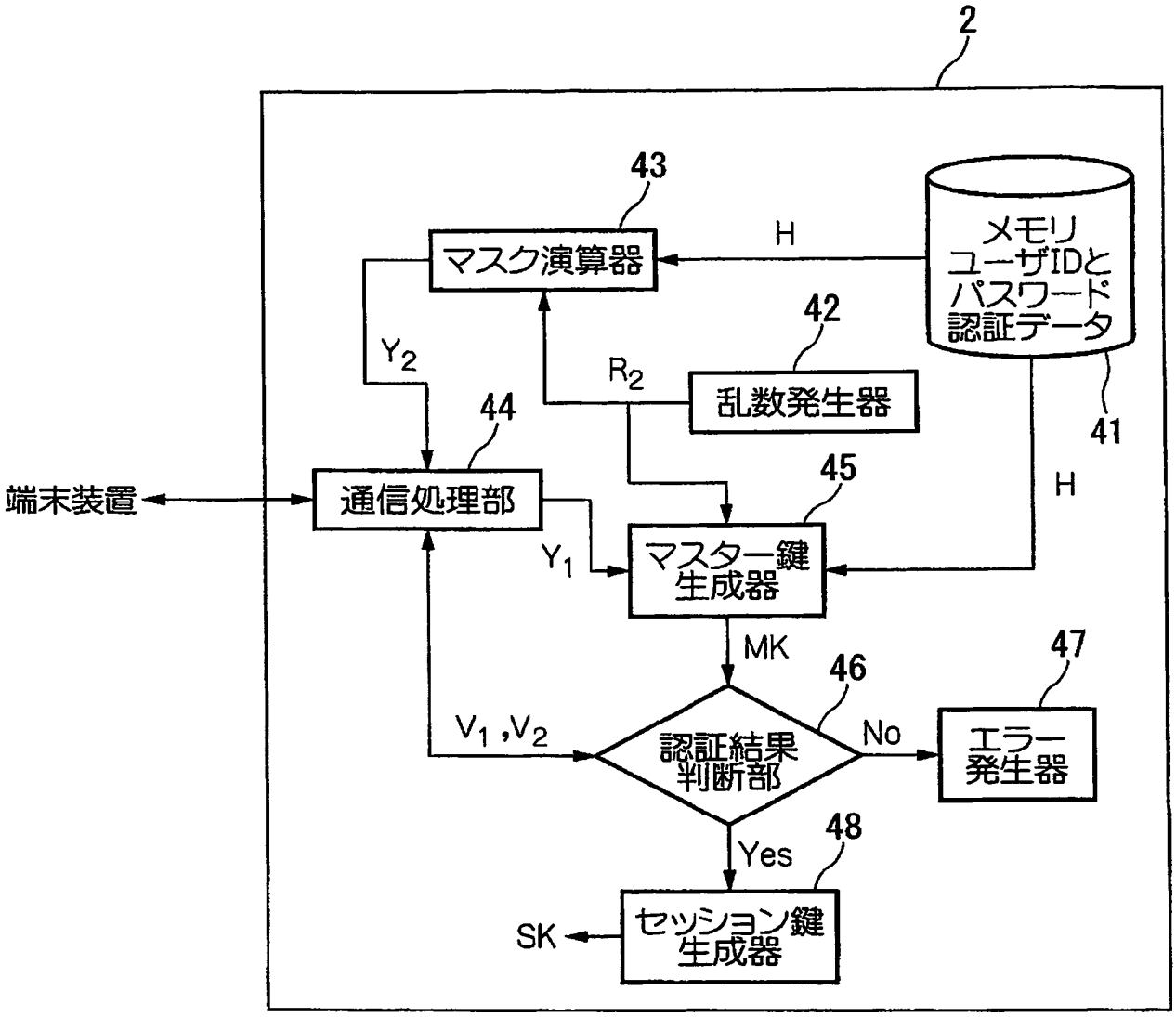


相互認証及び鍵交換

【図６】


サーバ
1
通信処理部
35
Y_1
Y_2
マスク演算器
34
V_1, V_2
SK
36
マスター鍵生成器
MK
37
認証結果判断部
Yes
39
セッション鍵生成器
No
38
エラー発生器
乱数発生器
33
R_1
12
メモリ
32
結合器
P
P'
パスワード入力

【図７】


2
43
マスク演算器
H
メモリ
ユーザIDと
パスワード
認証データ
42
乱数発生器
Y_2
R_2
44
41
端末装置
通信処理部
45
H
Y_1
マスター鍵
生成器
MK
47
46
V_1 ,V_2
認証結果
判断部
No
エラー
発生器
48
Yes
SK
セッション鍵
生成器

【書類名】要約書
【要約】
【課題】　情報の漏洩に強く、安全に暗号鍵の交換を行うことができる認証システムを提供する。
【解決手段】　端末装置とサーバ間において相互に認証を行う認証システムであって、ユーザのパスワードに基づいて、パスワード認証データＨと認証情報Ｐ’を求める処理と、求めた認証情報Ｐ’を予め記憶しておく処理と、記憶しておいた認証情報Ｐ’と認証時に入力されたパスワードを入力として所定の計算式により値Ｐを求める処理と、値Ｐと内部において発生させた乱数を入力として所定の計算式により値Ｙ１を求め、サーバへ送信する処理と、値Ｐと内部において発生させた乱数とサーバから受信した値Ｙ２を入力として所定の計算式により値ＭＫを求める処理と、値ＭＫを入力として所定の計算式により値Ｖ１を求め、サーバへ送信するとともに、サーバから受信した値Ｖ２と値Ｖ１と比較照合し、一致した場合にサーバを認証する処理とを有する。
【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－３６７５２７
受付番号	５０３０１７８６４６６
書類名	特許願
担当官	小池　光憲　　６９９９
作成日	平成１５年１０月３０日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 801000049
- 【住所又は居所】 東京都目黒区駒場四丁目６番１号
- 【氏名又は名称】 財団法人生産技術研究奨励会

【代理人】 申請人
- 【識別番号】 100064908
- 【住所又は居所】 東京都中央区八重洲２丁目３番１号　志賀国際特許事務所
- 【氏名又は名称】 志賀　正武

【選任した代理人】
- 【識別番号】 100108578
- 【住所又は居所】 東京都中央区八重洲２丁目３番１号　志賀国際特許事務所
- 【氏名又は名称】 高橋　詔男

【選任した代理人】
- 【識別番号】 100089037
- 【住所又は居所】 東京都中央区八重洲２丁目３番１号　志賀国際特許事務所
- 【氏名又は名称】 渡邊　隆

【選任した代理人】
- 【識別番号】 100101465
- 【住所又は居所】 東京都中央区八重洲２丁目３番１号　志賀国際特許事務所
- 【氏名又は名称】 青山　正和

【選任した代理人】
- 【識別番号】 100094400
- 【住所又は居所】 東京都中央区八重洲２丁目３番１号　志賀国際特許事務所
- 【氏名又は名称】 鈴木　三義

【選任した代理人】
【識別番号】　100107836
【住所又は居所】　東京都中央区八重洲２丁目３番１号　志賀国際特許事務所
【氏名又は名称】　西　和哉
【選任した代理人】
【識別番号】　100108453
【住所又は居所】　東京都中央区八重洲２丁目３番１号　志賀国際特許事務所
【氏名又は名称】　村山　靖彦

特願２００３－３６７５２７

出　願　人　履　歴　情　報

識別番号　［８０１０００００４９］

１．変更年月日　２００１年　８月３１日
［変更理由］　新規登録
住　所　東京都目黒区駒場四丁目６番１号
氏　名　財団法人生産技術研究奨励会